



Make Wireless Internet Security a Priority

Did you know that most new wireless routers come with no security settings? This makes your wireless connection available to anyone within range, which is especially important if you live in an apartment or condominium building. Someone could be using your Internet connection without your knowledge to conduct illegal or illicit activities.

Anyone that connects to your wireless network can potentially gain access to your computer and confidential information such as account numbers and passwords, email messages, etc. If there are people connecting to your network, your Internet service provider could hold you legally and financially responsible for any illegal activities that occur.

What Can You Do?

There are a few very simple settings that are easy to configure and provide a good base security to your wireless home network. Customers with a Wireless Cable Modem installed by SELCO will have these settings by default. It is recommended for all customers to use these settings as a minimum level of security on their wireless network.

1. **Change the default administrator password on your wireless access device.** *TIP:* Leave a sticky note on your wireless device with the password written down in case you forget what it is.
2. **Change the SSID to something unique.** SSID stands for *service set identifier* and is basically the name of your wireless device and the wireless network.
3. **Disable SSID broadcasting.** *TIP:* Write the SSID you chose on a piece of masking tape and put it on each of your computers so that you don't forget what you named your network once you have turned off broadcasting!



These are some very simple ways to protect your wireless home network. The steps for configuring these settings will vary depending on the manufacturer of your wireless device, but you may be able to find some simple instructions in the User's Guide or on their website.